CLAIM AMENDMENTS

1. (currently amended) A method of preventing the loss of confidentiality of electronically stored data in a computer system [[(11, 12, 13)]], which data in particular is organized as a data system [[(103)]] and or subdivided into blocks, in particular with use of exchangeable and/or removable data carriers and/or storage medium, where in particular peripherals are connectable to the computer system [[(11, 12, 13)]], characterized by the following steps:

analysis of the protocol and of the data stream [[(130, 131)]] from and to data carriers and/or storage media [[(104)]] and/or peripheral devices;

establishment of a classification, in particular for differentiation between nonremovable and removable data carriers and/or storage media [[(104)]];

determination on the basis of the established classification, whether an encryption of the electronically stored data is required for preventing the loss of confidentiality of the data and, depending on this determination, possibly

adding a cryptographic encryption [[(601, 602, 603)]] to the data system on a removable data carrier and/or a removable storage medium [[(104)]], [[and/]] or performing a cryptographic encryption on all or several blocks of the removable data carrier and/or of the removable storage medium [[(104)]].

2. (currently amended) The method according to claim 1, ~~characterized by~~ , further comprising the step of

determining that an encryption [[(105)]] of all blocks of the data carrier/storage medium [[(104)]] or an encryption [[(105)]] of all files [[(50)]] before storage on the data carrier/storage medium [[(104)]] and that an encryption [[(105)]] of several files [[(50)]] before storage on the data carrier /storage medium [[(104)]] is carried out.

3. (currently amended) The method according to claim 1 ~~or 2, characterized in that~~ wherein a cryptographic encryption is added to each data system [[(103)]] on nonremovable [[and/]] or nonexchangeable data carriers [[and/]] or storage media [[(104)]].

4. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 3 wherein the cryptographic encryption [[(105)]] is temporarily suspended when particular features are shown.

5. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1 wherein when a data carrier [[and/]] or a storage medium [[(104)]] without data system [[are]] is used, an encryption of all blocks is carried out and access is prevented.

6. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1 wherein an encryption [[(105)]] is performed when removable data carriers and or removable storage media ~~(104), in particular floppy disks, memory sticks, CD-RW, DVD-RW and the like,~~ are used.

7. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1 wherein an encryption [[(105)]] is performed when removable data carriers [[and/]] or nonremovable storage media [[(104)]], [[and/]] or network based data carriers [[and/]] or network based storage media [[(104)]] are used.

8. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1 wherein when a data carrier [[and/]] or a storage medium [[(104)]] is connected to a multifunctional interface [[and/]] or a multifunctional bus, ~~in particular slot, USB-port, and the like,~~ the functionality of the interfaces [[and/]] or the buses is maintained and an encryption

[[(105)]] is only performed on [[the]] data streams [[(130, 131)]] that are further transmitted to the interface [[and/]] or the bus for storing the data.

9. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1, further comprising the steps of

performing an analysis of the interface [[and/]] or the bus to which a data stream [[(130, 131)]] shall be transmitted ~~is performed~~ and [[that]]

taking the analysis ~~is taken~~ into account for establishing the classification on the basis ~~of criteria that can be determined, in particular on the basis~~ of the physical connection [[and/]] or the properties of the devices.

10. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1 wherein cryptographic methods for encryption are applied ~~, in particular the Rijndael algorithm~~.

11. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1 wherein the encryption is performed in ~~several steps, in particular in that after performing~~ accordance with a first cryptographic method, ~~the~~

~~data encrypted by the first method~~ and thereafter is again encrypted by means of a second cryptographic method.

12. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1, further comprising the step of, during a reading process from a data carrier [[and/]] or storage medium [[(104)]] that is at least partially encrypted,

performing a decryption of the data ~~is performed~~.

13. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1, further comprising the step of

preventing encryption of the data by using hardware with an integrated key [[and/]] or by using a password [[and/]] or by recognizing and controlling biometric data of a user ~~, an encryption (105) of data can be prevented~~.

14. (currently amended) The method according to claim 13~~, characterized in that~~ , further comprising the step of

preventing the encryption ~~(105) can be prevented~~ only at predetermined times.

15. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1 wherein for the encryption [[(105)]], keys [[(300)]] are used that are formed by combination of different parts [[(301, 302, 303)]], whereby in particular several computer systems [[(11, 12, 13)]] can be combined in groups [[(10)]], the keys [[(300)]] of a group [[(10)]] of computer systems [[(11, 12, 13)]] having a common part [[(301)]] as well as a respective individual part [[(302)]].

16. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 15 wherein the key [[(300)]] that is to be applied for the encryption and decryption [[(105)]] can be determined [[and/]] or stored in a data base for being requested [[and/]] or is integrated in a hardware [[and/]] or is determined from biometric data of a user by using an algorithm.

17. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1 wherein actions that are performed by means of the computer system ~~(11, 12, 13), such as storing and/or reading of data,~~ are recorded.

18. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1 wherein the computer system [[(11, 12, 13)]] has an operating system that at least distinguishes between a kernel mode [[(100)]] and a user mode [[(200)]], the method being at least partially implemented in the kernel mode [[(100)]].

19. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1 wherein a logic combination of several computer systems [[(11, 12, 13)]] within a group [[(10)]] is performed, wherein within the group [[(10)]] the cryptographic encryption [[(105)]] is mutually suspended, wherein the cryptographic encryption [[(105)]] is maintained with respect to external sources.

20. (currently amended) The method according to ~~one of the preceding claims, characterized in that~~ claim 1 wherein during access on a data carrier [[and/]] or storage medium [[(104)]], it is determined whether an encryption [[(105)]] of all blocks of the data carrier/storage medium [[(104)]] or an encryption [[(105)]] of all files [[(50)]] on the data carrier/storage medium [[(104)]] or an encryption [[(105)]] of several files [[(50)]] is present, and that an encryption of the requested data is performed.